

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

SCOTT LINMAN, on behalf of himself and all others
similarly situated,

Plaintiff,

v.

MARTEN TRANSPORT, LTD,

Defendant.

OPINION and ORDER

22-cv-204-jdp

This proposed class action is about a data breach. Plaintiff Scott Linman applied for a job with defendant Marten Transport, Ltd., a trucking and logistics company. As part of the application, he was required to provide Marten with sensitive personal information, including his date of birth and social security number. Several years later, hackers gained access to Marten's servers and stole Linman's personal information. Linman now asserts several state-law claims against Marten, contending that Marten failed to take reasonable measures to protect his data. Marten moves to dismiss the case under Federal Rule of Civil Procedure 12(b)(1) for lack of standing and under Rule 12(b)(6) for failure to state a claim. Dkt. 13.

The court will grant the motion in part. Linman's efforts to mitigate the risk of identity theft are a concrete injury, so he has standing to sue for damages. But Linman does not have standing to seek an injunction because he does not identify any injunctive relief that would reduce the risks of harm related to the breach. Linman has stated a negligence claim against Marten, but his other causes of action will be dismissed for failure to state a claim.

BACKGROUND

The court draws the following facts from Linman’s complaint, Dkt. 1. In considering these motions to dismiss under Federal Rule of Civil Procedure 12(b), the court accepts all factual allegations in the complaint as true and draws all reasonable inferences in favor of the plaintiff. *Bultasa Buddhist Temple of Chi. v. Nielsen*, 878 F.3d 570, 573 (7th Cir. 2017) (subject-matter jurisdiction); *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (failure to state a claim).

Linman applied for a position with Marten in 2018. As part of his job application, Linman was required to provide Marten with his name, address, date of birth, social security number, as well as his “financial information.” Dkt. 1, ¶ 60. (Linman does not specify what the financial information was.) Linman ultimately declined a job offer from Marten, but Marten continued to store Linman’s information on its servers.

About three years later in fall 2021, a group of hackers gained access to Marten’s servers. In March 2022, Marten notified Linman that his personal information had been “improperly accessed and/or obtained by unauthorized third parties.” *Id.* The notice stated that Linman’s social security number was “compromised” as a result of the breach. *Id.*

Linman has spent about two hours on activities meant to mitigate the risk of identity theft, including reviewing his credit report and signing up for credit monitoring service. Linman alleges that, as a result of the breach, his debit card information was accessed and used by unauthorized third parties in March 2022. *Id.*, ¶ 62.

The court will discuss additional facts in the analysis section of the opinion.

ANALYSIS

A. Subject matter jurisdiction

Neither party challenges jurisdiction on grounds other than standing, but courts have an independent obligation to ensure that jurisdiction is proper. *See Ware v. Best Buy Stores, L.P.*, 6 F.4th 726, 731 (7th Cir. 2021) Linman relies solely on 28 U.S.C. § 1332(d) as a basis for jurisdiction. That statute applies to a proposed class action that meets the following criteria: (1) the proposed class includes at least 100 members; (2) at least one member of the class is a citizen of a state different from any defendant; and (3) the aggregated amount in controversy is more than \$5 million. *See Ware*, 6 F.4th at 733.

Linman seeks to represent a nationwide class composed of “[a]ll United States residents whose [personally identifiable information] was or could have been accessed” during the breach. Dkt. 1, ¶ 67. Linman alleges that approximately 35,000 individuals had their data exposed in the breach, *id.*, ¶ 6, so it appears that the proposed class includes at least 100 members. The diversity requirement is met because Linman alleges that he is a citizen of Arizona and Marten is a citizen of Wisconsin.

As for the amount in controversy, Linman alleges only that “the amount of [sic] controversy exceeds the sum or value of \$5 million.” *Id.*, ¶ 19. That conclusory statement alone isn’t enough to meet the amount in controversy requirement. *See Ware*, 6 F.4th at 732. Nevertheless, the court is satisfied that the amount in controversy plausibly exceeds \$5 million. With an estimated 35,000 members in the class, the amount in controversy would exceed \$5 million if each class member, on average, could recover \$143 in damages. Linman alleges that the class has suffered harms including actual identity theft, time spent mitigating the risk of identity theft, and credit monitoring expenses. The Seventh Circuit has observed in other

cases involving data breaches that credit monitoring services can cost up to \$19.95 a month, *see Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015), so it is plausible that class members could incur over \$143 in monitoring expenses. *See In re TJX Companies Retail Sec. Breach Litig.*, 584 F. Supp. 2d 395, 400 (D. Mass. 2008) (approving class settlement for victims of retail security breach in which it was estimated that three years of credit monitoring would cost \$390); *cf. Bohnenstiehl v. McBride, Lock, & Assocs., LLC*, No. 16-CV-306-NJR-DGW, 2016 WL 6872955 (S.D. Ill. Nov. 22, 2016) (concluding that credit monitoring expenses of \$22,000 for each class member was implausible).

The court is satisfied that jurisdiction is proper, so it will turn to Marten's motion to dismiss.

B. Motion to dismiss

Linman asserts state-law claims for negligence, breach of implied contract, unjust enrichment, invasion of privacy, and breach of confidence against Marten. Marten moves under Federal Rule of Civil Procedure 12(b)(1) to dismiss the case for lack of standing and moves to dismiss under Rule 12(b)(6) for failure to state a claim.

1. Standing

Plaintiffs must demonstrate standing for each of their claims and for each form of relief that they seek. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021). To establish standing, a plaintiff must show that he (1) suffered an injury in fact that is (2) fairly traceable to the challenged conduct of the defendant and (3) likely to be redressed by a favorable judicial decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). Marten contends that Linman cannot establish the first two elements.

“To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (internal quotation marks omitted). A substantial risk of future harm is a concrete injury for the purposes of injunctive relief. *TransUnion*, 141 S. Ct. at 2210; *Ewing v. Med-I Sols., LLC*, 24 F.4th 1146, 1151 (7th Cir. 2022). But “a risk of future harm, without more, is insufficiently concrete to permit standing to sue for damages in federal court.” *Ewing*, 24 F.4th at 1151. Linman seeks both damages and an injunction, so he must show that he has standing to seek each type of relief.

a. Damages

Linman contends that he has identified five distinct concrete injuries that give him standing to sue for damages: (1) the fraudulent charges on his debit card; (2) the threat of future identity theft; (3) time spent mitigating that threat; (4) a loss of privacy; and (5) anxiety and emotional distress. Marten does not dispute that the fraudulent charges are a concrete harm, but it contends that they are not fairly traceable to the breach. As for the other alleged injuries, Marten does not dispute that they are fairly traceable to the breach, but it contends that those injuries are not concrete.

The court concludes that Linman’s time spent mitigating the risk of identity theft is a concrete harm that gives him standing to sue for damages related to the breach, so the court need not consider whether the other alleged injuries are sufficient. Even an “identifiable trifle” can constitute an injury in fact. *Craftwood II, Inc. v. Generac Power Sys., Inc.*, 920 F.3d 479, 481 (7th Cir. 2019) (holding that the time lost reading a junk fax before discarding it is a concrete injury) (quoting *United States v. SCRAP*, 412 U.S. 669, 689 n.14 (1973)). Plaintiffs “cannot

manufacture standing by incurring costs in anticipation of non-imminent harm,” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 401 (2013). But time and effort spent on reasonable mitigation efforts are a concrete injury if the harm is imminent. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

In cases with similar facts to this one, the Seventh Circuit has concluded that the theft of sensitive personal information presents an imminent threat of identity theft. *See id.* at 694; *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016). Here, Linman alleges not only that his personal data was exposed, but that hackers accessed and downloaded it. It was reasonable for Linman to spend time mitigating the risk of identity theft under those circumstances. *See Lewert*, 819 F.3d at 967 (time plaintiff spent “monitoring both his card statements and his other financial information as a guard against . . . identity theft” was a concrete injury.)

Marten contends that time spent mitigating a risk of harm cannot be a concrete injury, citing the Supreme Court’s recent decision in *TransUnion LLC v. Ramirez*. In that case, the Court clarified that a risk of future harm, without more, is not a concrete injury for a damages suit. 141 S. Ct. at 2200; *Ewing*, 24 F.4th at 1152 (construing *TransUnion*). Marten contends that if a risk of harm cannot be a concrete injury, time spent mitigating that risk cannot be a concrete injury, either.

This court is not persuaded. *TransUnion* did not address whether time spent mitigating a risk is a concrete harm, and there is no indication that the plaintiffs in that case argued that they had standing on that ground. In any event, Marten’s argument does not follow from *TransUnion*’s holding. The Court in *TransUnion* emphasized that whether a harm is concrete turns on whether it had already occurred. Injuries that had occurred were concrete; but injuries

that *could* materialize were too speculative to support a damages suit. *See TransUnion*, 141 S. Ct. at 2211–12. Here, Linman has already lost time mitigating the risk of identity theft. That injury is not speculative because he has already suffered it.

Moreover, *TransUnion* does not say that an injury is speculative merely because it is related to a risk of harm. The Seventh Circuit has construed *TransUnion* to stand for the proposition that “a risk of future harm, *without more*, is insufficiently concrete” for a damages suit. *Ewing*, 24 F.4th at 1152 (emphasis added). And in *TransUnion* itself, the Court endorsed defendants’ argument that a risk of harm is not concrete “unless the exposure to the risk of future harm itself causes a *separate* concrete harm.” *TransUnion*, 141 S. Ct. at 2210–11 (emphasis in original). The time spent mitigating the risk of identity theft is a separate harm from the risk of identity theft itself. Marten’s argument would deny any relief to plaintiffs who made reasonable efforts to mitigate an imminent risk of harm so long as that risk did not materialize, even if the risk was created by the defendant. That result does not follow from *TransUnion*, so the court concludes that Linman has standing to sue for damages.

b. Injunctive relief

A plaintiff has standing to seek injunctive relief if he faces an “imminent and substantial” risk of future harm. *TransUnion*, 141 S. Ct. at 2210. For the reasons explained above, it is plausible to infer that the theft of a social security number gives rise to an imminent and substantial risk of identity theft. *See Remijas*, 794 F.3d at 693.

Marten contends that Linman does not have standing to seek injunctive relief because none of the injunctive relief Linman seeks would reduce the risk of identity theft. Nearly all of Linman’s requested injunctive relief is about how Marten will handle its data in the future: he seeks to order Marten to, among other things, prohibit Marten from maintaining his personal

information on a cloud-based database; engage in periodic security audits; improve security training; and monitor the traffic to and from its servers. Dkt. 1, at 39–40.

Marten frames this argument in terms of whether Linman’s harm is concrete, but it is really about redressability, the third element of standing. For a risk of harm to be redressable, a plaintiff must show that the risk of harm “would be reduced to some extent if [plaintiff] received the relief [he] seek[s].” *Massachusetts v. E.P.A.*, 549 U.S. 497, 526 (2007). None of the relief Linman seeks would reduce the risk of harm that hackers will misuse information that has already been stolen, and nothing in Linman’s complaint suggests that Marten is at risk of future data breaches.

Linman did not respond to this argument in any way, such as by identifying any particular injunctive relief he is seeking that will decrease the risk of identity theft stemming from the breach. By failing to respond to Marten’s argument, Linman has conceded that he does not have standing to seek injunctive relief. *Bonte v. U.S. Bank, N.A.*, 624 F.3d 461, 466 (7th Cir. 2010) (failing to respond to argument constitutes waiver); 13 C. Wright, A. Miller & E. Cooper, *Federal Practice & Procedure* § 3522, at n.17 (3d ed.) (“Though subject matter jurisdiction cannot be established by waiver or estoppel, it can be defeated by them.”) The court will dismiss Linman’s requests for injunctive relief for lack of standing.

2. Failure to state a claim

Linman asserts state-law claims for negligence, breach of implied contract, invasion of privacy, “breach of confidence,” and unjust enrichment. Marten moves to dismiss all of Linman’s claims for failure to state a claim. Linman does not identify which state’s law he is suing under. Marten assumed in its brief that Wisconsin law applies, and Linman did not challenge that assumption. If the parties do not raise any choice of law issues, the law of the

forum state applies. *FutureSource LLC v. Reuters Ltd.*, 312 F.3d 281, 283 (7th Cir. 2002). So the court will apply Wisconsin law.

1. Negligence

In Wisconsin, negligence has four elements: (1) a duty of care; (2) a breach of that duty; (3) a causal connection between the conduct and the injury; (4) an actual loss or damage as a result of the injury. *Dixon ex rel. Nikolay v. Wisconsin Health Organization Insurance Corp.*, 2000 WI 95, P 21, 237 Wis. 2d 149, 612 N.W.2d 721. Marten challenges only the fourth element, contending that Linman has not alleged that he suffered damages as a result of the breach. But “[Federal] Rule [of Civil Procedure] 8 does not create a pleading standard for damages beyond what is necessary to establish standing.” *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 795 (W.D. Wis. 2019). “To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available.” *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). The court has determined that Marten has alleged an injury in fact, so Linman’s allegations are sufficient to state a claim for negligence.

2. Breach of implied contract

For a contract to exist, there must be an offer, acceptance, and consideration. *Goossen v. Estate of Standaert*, 189 Wis. 2d 237, 247, 525 N.W.2d 314 (Ct. App. 1994). An implied contract is a contract established by the conduct of the parties, without an express written or oral agreement. *See Hydro Well Drilling LLC v. Ryan*, 2018 WI App 66, 384 Wis. 2d 415, 921 N.W.2d 531. To recover on an implied contract, the plaintiff must prove three things: (1) the defendant requested the plaintiff to perform services; (2) the plaintiff complied with the request; and (3) the services were valuable to the defendant. *Ostrenga Excavating, Inc. v. Cleveland*

Constr., Inc., 2017 WI App 80, 378 Wis. 2d 739, 905 N.W.2d 843. These elements make a prima facie showing that the defendant promised to pay the plaintiff for the services. *Id.* Put another way, those circumstances “show a mutual intention to contract.” *Piaskoski & Assocs. v. Ricciardi*, 2004 WI App 152, ¶17, 275 Wis. 2d 650, 686 N.W.2d 675.

Linman alleges that Marten agreed to take reasonable measures to protect his data in exchange for providing Marten with his personal information. As the source of Marten’s obligation, Linman identifies the privacy policy on Marten’s website, which states (in relevant part) that it “exercise[s] great caution and great care in providing secure transmission of your information from your PC to our servers” and that Marten makes its “best effort to ensure its security on [its] systems.” Dkt. 1, ¶¶ 26, 42.

Linman has not shown that he had a contract with Marten. Although Linman states that he was required to provide his information as part of a job application, he does not allege that Marten directed him to apply for the job. And his decision to submit an application did not provide a valuable service to Marten.

Linman cites several cases where privacy policies similar to the one on Marten’s website gave rise to an implied contract claim. But in those cases, the promise to protect the plaintiffs’ data was part of a broader contractual relationship between the parties: specifically, employee-employer, *see Sackin v. Transperfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 (S.D.N.Y. 2017), or customer-merchant, *Fox*, 399 F. Supp. 3d at 801; *In re Marriott Int’l, Inc.*, 440 F. Supp. 3d 447, 484 (D. Md. 2020). In those cases, the plaintiffs provided defendants with valuable consideration—money or labor—as part of their express contractual relationship, and the promise to protect plaintiffs’ data arose from that contract. *See Sackin*, 278 F. Supp. 3d at 750 (“TransPerfect required and obtained the PII as part of the employment relationship”);

Fox, 399 F. Supp. 3d at 801 (reasonable to infer that the parties “intended to incorporate the policy into their contract for health services”); *Irwin v. Jimmy John’s Franchise, LLC*, 175 F. Supp. 3d 1064, 1070 (C.D. Ill. 2016) (“There is an implicit agreement to safeguard the customer’s information to effectuate the contract.”). The cases Linman relies on don’t suggest that a company’s privacy policy, standing alone, creates an implied contract to protect personal information.

Linman doesn’t allege facts suggesting that he had a contractual relationship with Marten similar to a customer’s or an employee’s. Linman did not pay Marten for its services or provide Marten with labor. Linman contends that an applicant’s personal information is valuable because it gives the employer the ability to hire the applicant. But he provides no authority for that proposition, and he cites no cases acknowledging a contractual relationship between applicants and potential employers. His breach of implied contract claim will be dismissed.

3. Unjust enrichment

Under Wisconsin law, the elements of an unjust enrichment claim are: (1) a benefit conferred by the plaintiff to the defendant; (2) defendant’s knowledge of the benefit; and (3) it would be inequitable for defendant to retain the benefit without paying its value. *Admiral Ins. Co. v. Paper Converting Mach. Co.*, 2012 WI 30, 339 Wis. 2d 291, 811 N.W.2d 351.

Linman has not stated an unjust enrichment claim because he identifies no benefit that his personal information provided Marten. “Unjust enrichment generally refers to a monetary benefit conferred upon a defendant.” *Reetz v. Advoc. Aurora Health, Inc.*, 2022 WI App 59, ¶ 29, 405 Wis. 2d 298, 326, 983 N.W.2d 669, 683. Here, there is no allegation that Marten realized a monetary benefit from Linman’s data. He does not allege that Marten sold his data or that

Marten received payment to store it. *Cf. In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412 (E.D. Va. 2020) (concluding that Amazon “profited from its storage and retention of Plaintiffs’ [personal information]” because it received fees to do so). A merchant may be unjustly enriched if a customer would have paid less for a service had he known that his data would not be secure. *See Fox*, 399 F. Supp. 3d at 802. But Linman does not allege that he purchased anything from Marten. The court will dismiss Linman’s unjust enrichment claim.

4. Invasion of privacy

In Wisconsin, torts related to the invasion of privacy are codified under Wisconsin Statute § 995.50. Linman does not identify which cause of action he is suing under, but he contends that his claim is best understood as a claim for “intrusion upon seclusion.” Dkt 15, at 23. The closest statutory analogue for that tort is codified at Wisconsin Statute § 995.50(2)(am)1. *See Hillman v. Columbia Cty.*, 164 Wis. 2d 376, 391, 474 N.W.2d 913, 919 (Ct. App. 1991). That section of the statute defines invasion of privacy as an “[i]ntrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.” Wis. Stat. § 995.50(2)(am)1. The Wisconsin Court of Appeals has concluded that a defendant need not act “with a particular mental state or intent” for there to be a valid cause of action under this section of the statute. *Gillund v. Meridian Mut. Ins. Co.*, 2010 WI App 4, ¶ 29, 323 Wis. 2d 1, 20, 778 N.W.2d 662, 672; *see also Reetz*, 2022 WI App 59, ¶ 21 n.9.

Linman hasn’t stated a claim for intrusion upon seclusion for one simple reason: it was the hackers, not Marten, that intruded on Linman’s privacy. Linman provided his personal information to Marten willingly, so it didn’t intrude on his privacy by collecting it. The only “intrusion” was the alleged breach by the hackers. *See Mitchell v. USDA Farm Serv. Agency*, No.

13-cv-500-bbc, 2014 WL 7240671, at *3 (W.D. Wis. Dec. 17, 2014) (dismissing claim because plaintiff did “not allege[] that defendant gained access to the information by trespassing or intruding.”).

Linman contends that other district courts have allowed plaintiffs to proceed on similar claims in data breach cases, citing *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 819 (E.D. Ky. 2019) and *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-00186-CHB, 2021 WL 3076786, at *4 (W.D. Ky. July 1, 2021). But those cases are distinguishable. In *McKenzie* and *Savidge*, an employee of the defendant released employee tax information to cybercriminals in response to a phishing email. *McKenzie*, 369 F. Supp. at 814; *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-186-CHB, 2020 WL 265206, at *1 (W.D. Ky. Jan. 17, 2020) (discussing plaintiffs’ allegations in greater detail). The court in *McKenzie* concluded that the company had intruded on plaintiffs’ privacy because the employee “took an affirmative action to gather the tax information for [defendant’s] employees” prior to sending it. *Id.* at 819. It appears that the defendant in *Savidge* did not dispute that it had intruded on plaintiffs’ privacy, so the court did not address that issue. *See* 2021 WL 3076786, at *3. But the court in *Savidge* cited *McKenzie* approvingly and concluded that the plaintiffs in *Savidge* had stated a claim for the same reasons that the *McKenzie* plaintiffs did. *Id.* at *4.

Here, Linman does not allege that a Marten employee intruded on his privacy by taking affirmative action to gather his personal information. Rather, he alleges that hackers gained access to Marten’s servers and downloaded his personal information directly. The court will dismiss his invasion of privacy claim.

5. Breach of confidence

Linman asserts a claim for “breach of confidence,” alleging that Linman gave his private information to Marten with the expectation that Marten would take reasonable efforts to protect it. Marten contends that Wisconsin does not recognize a cause of action for breach of confidence distinct from an invasion of privacy claim. Linman cites no authority to dispute that contention. Some federal courts applying Wisconsin law have stated that the concept of “breach of confidentiality” is relevant to trade secret claims, see *Metso Minerals Indus., Inc. v. FLSmidth-Excel LLC*, 733 F. Supp. 2d 969, 973 (E.D. Wis. 2010), and professional negligence claims where the defendant owed the plaintiff a duty of confidentiality, see *Smith v. Dep’t of Corr. of State of WI*, No. 03 C 0103, 2005 WL 2449841, at *24 (E.D. Wis. Sept. 30, 2005). But Linman cites no cases—and this court has found none—where a Wisconsin court recognized an independent claim for “breach of confidence.” This claim will be dismissed.

C. Leave to amend

Linman asks for leave to amend his any portion of the complaint that is dismissed. The court will deny the request as futile. Linman’s breach of confidence claim is not a recognized cause of action under Wisconsin law. As for his breach of contract, unjust enrichment, and invasion of privacy claims, it is hard to see how Linman could allege additional facts consistent with his original complaint that state claims for relief. Linman does not explain what information he could plead to show that his job application was valuable to Marten or that Marten intruded on his privacy. If Linman believes that amendment would not be futile, he may file a separate motion for leave to amend that (1) identifies specific information that was unavailable to him at the time he drafted his complaint and (2) explains why it entitles him to a different result.

D. Request to strike

Marten requests to strike paragraphs 45–53 of Linman’s complaint that contain general information about identity theft and information security because they are not about Linman’s personal experiences. Dkt. 14, at 19. Motions to strike are disfavored because “striking a portion of a pleading is a drastic remedy and because it is often sought by the movant simply as a dilatory tactic.” *Riemer v. Chase Bank, N.A.*, 275 F.R.D. 492, 494 (N.D. Ill. 2011). The court will not grant a motion to strike unless the challenged allegations have no possible relation to the controversy and are clearly prejudicial. *Kundinger v. NRRM, LLC*, No. 17-cv-321-jdp, 2017 U.S. Dist. LEXIS 182514, at *2 (W.D. Wis. Nov. 3, 2017). The allegations establish the potential risks of the breach to Linman, and Marten does not explain why the allegations would be confusing to the court or to a jury. The request is denied.

ORDER

IT IS ORDERED that defendant Marten Transport’s motion to dismiss, Dkt 13, is GRANTED in part. Plaintiff Scott Linman’s claims for injunctive relief, breach of contract, unjust enrichment, invasion of privacy, and breach of confidence are DISMISSED. The motion is denied as to Linman’s negligence claim.

Entered March 17, 2023.

BY THE COURT:

/s/

JAMES D. PETERSON
District Judge